

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 7,050,579 B1
APPLICATION NO. : 09/558138
DATED : May 23, 2006
INVENTOR(S) : Koç et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page under Other Publications on Page 2, second Col. line 9, "GF(2^m)"
should read -- GF(2^m) --

Column 6, line 38, " $k \leq m$ " should read -- $k \geq m$ --

Column 6, line 52, " a^{-1} " should read -- a^{-1} --

Column 9, line 10, " $U=T^0$ " should read -- $U=T^e$ --

Signed and Sealed this

Twenty-eighth Day of November, 2006

A handwritten signature in black ink, appearing to read "Jon W. Dudas". The signature is stylized with a large, looped initial "J" and a distinct "D" at the end.

JON W. DUDAS
Director of the United States Patent and Trademark Office